

---

Date: May 17, 2023

To: Yeman Collier, Vice President, and Chief Information Officer  
Michael Schnabel, AVP, Information Security & Operations (CISO)

From: John Lazarine, Chief Audit Executive  
Internal Audit & Consulting

Subject: Audit Report – *Audit of Azure Virtual Desktop*

---

As part of our FY 2023 Audit Plan, we completed an audit of *Azure Virtual Desktop*. Attached is the report detailing the results of this review. Management’s Action Plans are included in the section – “Summary of the Audit of Azure Virtual Desktop”, of the report.

We appreciate the cooperation and assistance we received from Information Security Team throughout the review.

Respectfully,



John Lazarine, CIA, CISA, CRISC  
Chief Audit Executive  
Internal Audit & Consulting Services

Distribution:

cc: Dr. William Henrich, President  
Andrea Marks, Senior Executive Vice President, and Chief Operating Officer  
Ginny Gomez-Leon, Vice President, and Chief Financial Officer  
Todd Holling, Deputy Chief Information Officer  
Chuntida Harinnitisuk, Director, Director Enterprise Systems & Operations  
J. Michael Peppers, Chief Audit Executive, UT System

External Audit Committee Members:

Randy Cain  
Carol Severyn  
Ed Garza

## Executive Summary

### Background

Azure Virtual Desktop (AVD) is a desktop and app virtualization service that runs on the cloud. In response to an increasing number of remote users, campus outages, and hardware supply chain delays, AVD makes it easier and quicker for users to work remotely from any device or location.

AVD implementation is an ongoing project with a tentative go-live timeline in May 2023.

At Management's request, an assessment was performed at the "Testing and Validation" phase of the implementation to ensure,

- AVD configuration settings were enabled accordingly per the industry's best practices and aligned with UTHSCSA's IT Security policy,
- Users assigned privileged IT access were appropriate based on their job functions prior to go-live.

### Objective & Scope

We assessed Azure Virtual Desktop at UT Health San Antonio during the preparation for going live into production. The primary objective of the audit was to determine the security baseline for Azure Virtual Desktop regarding configuration settings and user privileges in the institution's network computing environment was suitably designed and operated effectively.

The scope of the audit was to determine the appropriateness of the enabled AVD security configuration settings with regard to the industry's best practices and user privileges in the system prior to go-live. The control domains covered in the assessment are listed below.

- Network Security - *Network Security covers controls to secure and protect networks, including securing virtual networks, establishing private connections, preventing, and mitigating external attacks, and securing DNS.*
- Identity Management - *Identity Management covers controls to establish a secure identity and access controls using identity and access management systems, including the use of single sign-on, strong authentications, managed identities (and service principals) for applications, conditional access, and account anomalies monitoring.*
- Privileged Access - *Privileged Access covers controls to protect privileged access to your tenant and resources, including a range of controls to protect your administrative model, administrative accounts, and privileged access workstations against deliberate and inadvertent risk.*
- Data Protection - *Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discovering, classifying, protecting, and monitoring sensitive data assets using access control, encryption, key management and, certificate management.*
- Asset Management - *Asset Management covers controls to ensure security visibility and governance over your resources, including recommendations on permissions for security personnel, security access to asset inventory, and managing approvals for services and resources (inventory, track, and correct).*
- Logging and Threat Detection - *Logging and Threat Detection cover controls for detecting threats on the cloud, and enabling, collecting, and storing audit logs for cloud services, including enabling detection, investigation, and remediation processes with controls to generate high-quality alerts with native threat detection in cloud services; it also includes collecting logs with a cloud monitoring service, centralizing security analysis with a SIEM, time synchronization, and log retention.*

- Posture and Vulnerability Management - *Posture and Vulnerability Management focus on controls for assessing and improving the cloud security posture, including vulnerability scanning, penetration testing, and remediation, as well as security configuration tracking, reporting, and correction in cloud resources.*
- Endpoint Security - *Endpoint Security covers endpoint detection and response controls, including endpoint detection and response (EDR) and anti-malware service for endpoints in cloud environments.*
- Backup and Recovery - *Backup and Recovery covers controls to ensure that data and configuration backups at the different service tiers are performed, validated, and protected.*
- Entity Level Controls - *Entity Level covers controls that help ensure that the entire entity's management directives are carried out.*

We conducted our audit in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The audit is also intended to meet the TAC 202<sup>1</sup> biennial review, as required by the State of Texas and UT System Administration.

### **Summary of Results**

The AVD assessment was completed prior to go-live implementation of the system. This was to ensure configuration settings were enabled accordingly based on best practice and elevated privileged access were appropriate. Based on our evaluation, the following control domains were suitably designed and operated effectively:

- Network Security
- Asset Management
- Logging and Threat Detection
- Posture and Vulnerability Management
- Endpoint Security

However, opportunities were identified that present elevated risks that should be addressed prior to go-live to ensure processes and controls are adequately designed and in place.

The data at risk includes, but is not limited to, patient health records and billing information.

Based on the completed assessment, the summary of noted findings is categorized in the area of impacted control domains. These are:

- Identity Management - *There was no monitoring control in place to address the risk of accidental or intentional inappropriate use of access or unauthorized changes in the system. Also, there was no established approval process and access path for requesting and approving vendor support requests and temporary access to data through a secured channel.*
- Privileged Access - *Elevated privileged IT access was not restricted to authorized users based on their job roles and responsibilities. The risks of accidental or intentional inappropriate use of access or unauthorized changes in the system were not addressed.*
- Data Protection - *The configuration setting was not enabled to support data-at-rest encryption using the customer-managed keys for the institution's content stored by the service. As such, the risk of inconsistently executing changes to data in the production environment due to ill-defined procedures was not addressed. The data at risk includes, but is not limited to, patient health records and billing information.*
- Backup and Recovery - *There was no established process for backup and recovery. The risk of hardware and software issues resulting in loss of data or the inability to access data as required was not addressed.*
- Entity Level Controls - *There was no review of the SOC 2 Type 2 report for Azure Virtual Desktop performed by management.*

Although, these finding exist today, the remediation is planned to be completed prior to system go-live. During this audit, and as noted in the report below, where feasible, management has already taken action to remediate some of the identified observations prior to go-live implementation.

---

<sup>1</sup> Texas Administrative Code Chapter 202 (TAC §202), RULE §202.76 (c) A review of the institution's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s).

Management has agreed with the results of this audit and to address the associated risk.

We would like to thank Information Security Team for the support and assistance provided during this audit.

#### **AUDIT TEAM**

Samuel Babajide, IT Audit Director, MSEM, CISA, CIPT, CPSP, ITIL

#### **APPROVED FOR RELEASE**



John Lazarine, Chief Audit Executive, Internal Audit & Consulting Services

#### **DISTRIBUTION**

Dr. William Henrich, President

Andrea Marks, Senior Executive Vice President, and Chief Operating Officer

Ginny Gomez-Leon, Vice President and Chief Financial Officer

Yeman Collier, Vice President, and Chief Information Officer

Michael Schnabel, AVP, Information Security and Operations (CISO)

Chuntida Harinnitisuk, Director, Enterprise Systems & Operations

Joel Gallegos, IT Systems Architect

J. Michael Peppers, Chief Audit Executive, UT System

#### **Criteria**

Texas Administrative Code Chapter 202 (TAC §202) outlines the minimum information security and cybersecurity responsibilities and roles at state agencies and institutions of higher education. TAC §202 requires agencies and institutions of higher education to use the TAC §202 Security Controls Standards Catalog (SCSC). The security controls catalog is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, R5, and the Control Objectives for Information and Related Technologies (COBIT). Using a centrally managed controls catalog effectively ensures that all agencies and institutions use common language and minimum standards when implementing security measures.

#### **Testing Methodology and Results**

Internal Audit utilized TAC §202 SCSC as part of the validation testing to determine controls were suitably designed and operating effectively. The results of the test work are summarized above:

- **(\*) Risk and Risk Ranking**
  - **Red** = High Risk
  - **Yellow** = Medium Risk
  - **Green** = Low Risk
- **Mitigating Control** (as defined in TAC §202 Security Controls Standards Catalog)
- **Control Status**
  - **Red** = Control is not in place and/or not working
  - **Yellow** = Control is in place and is not reliable
  - **Green** = Control is in place and operating effectively

## RISK RATING

<b>Priority</b>	An issue identified by an internal audit that, if not addressed on a timely basis, could directly impact the achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.
<b>High</b>	A finding identified by an internal audit that is considered to have a medium to high probability of adverse effects to a UT institution or UT System as a whole.
<b>Medium</b>	A finding identified by an internal audit that is considered to have a low to medium probability of adverse effects to a UT institution or UT System as a whole.
<b>Low</b>	A finding identified by an internal audit that is considered to have minimal probability of adverse effects to a UT institution or UT System as a whole.
<b><i>n/a</i></b>	No reportable findings or observations were identified during the course of the audit.

*Summary of the Audit of Azure Virtual Desktop  
Issues & Recommendation*




















#	Observation/ Condition	Risk	Risk Rating	Recommendation	Management's Response
1	<p><b><u>Identity management</u></b></p> <p>(a) There is no privileged access activity monitoring process in place.</p> <p>(b) There is no established approval process and access path for requesting and approving vendor support requests and temporary access to data through a secure channel.</p>	<p>Information in applications is accessed by users and other personnel outside of defined business requirements.</p>	<p>High</p>	<p>(a) Management to ensure elevated privileged access activities captured in the audit log are reviewed annually.</p> <p>(b) An established approval process and access path for requesting and approving vendor support requests and temporary access to data through a secure channel should exist.</p>	<p>a) Develop an annual report to audit elevated access within Subscriptions and management tools. The report will identify the user and role within the subscription and management tool. Management will determine if permission should be maintained or revoked. The second report will be created to look for anomalies to identify elevated access that has been provisioned before the annual report has been reviewed.</p> <p>b) A support process and approval workflow will be created to determine if vendor access to data is needed. If access is needed workflow includes approval and revoking steps.</p> <p><b>Target Date</b> – 05/01/2023</p> <p><b>Remediation Owner</b> – Joel Gallegos, IT System Architect.</p> <p><b>Control Deficiency Remediated.</b></p>






2	<p><b><u>Privileged Access</u></b></p> <p>2 of 6 Intune administrators and 1 of 2 User Administrator accounts, considered privileged administrative accounts, were independently evaluated by Internal Audit and confirmed by management as inappropriate.</p>	<p>Accidental or intentional inappropriate use of access or unauthorized changes in the system.</p>	<p>High</p>	<p>Management to ensure elevated privileged access is assigned on a least privileged basis and restricted to a limited number of individuals based on their job roles and responsibilities</p>	<p>Develop an annual report to audit elevated access within Subscriptions and management tools. The report will identify the user and role within the subscription and management tool. Management will determine if permission should be maintained or revoked. The second report will be created to look for anomalies to identify elevated access that has been provisioned before the annual report has been reviewed.</p> <p><b>Target Date</b> – 05/01/23</p> <p><b>Remediation Owner</b> - Joel Gallegos, IT System Architect.</p> <p><b>Control Deficiency Remediated.</b></p>
3	<p><b><u>Data Protection</u></b></p> <p>To determine whether the Service supports data-at-rest encryption using customer-managed keys is supported for customer content stored by the service, IA noted configuration was enabled for "Microsoft managed key".</p>	<p>Changes to data are executed inconsistently in the production environment due to ill-defined procedures.</p>	<p>High</p>	<p>Configuration settings should be updated to use "customer-managed keys to support data-at-rest encryption.</p>	<p>Customer-managed keys for the Azure storage account have been created and we are in the process to deploy to the storage account. A policy has also been created to audit if the storage account is not configured with Customer managed keys.</p> <p>This is in testing phase.</p> <p><b>Target Date</b> – 05/19/23</p> <p><b>Remediation Owner</b> - Joel Gallegos, IT System Architect.</p>
4	<p><b><u>Backup and Recovery</u></b></p> <p>There is no established backup and recovery process.</p>	<p>Hardware and software issues result in loss of data or the inability to access data as required.</p>	<p>Medium</p>	<p>(a) A backup and recovery process should be put in place. (b) The backup tool should be configured to notify authorized individuals when a backup failure occurs.</p>	<p>The second phase of Azure Virtual Desktop will include a scope for backup and recovery. The process will be developed to meet SLA identified.</p> <p><b>Target Date</b> – 05/01/23</p> <p><b>Remediation Owner</b> - Joel Gallegos, IT System Architect</p> <p><b>Control Deficiency Remediated.</b></p>



	<p><b><u>Entity Level Controls</u></b></p> <p>There was no review of the SOC 2 Type 2 report for Azure performed by management.</p>	<p>Failing to review your vendor's SOC report means that you won't know whether key controls were identified and audited. Additional evidence might be required if these controls weren't included.</p>	<p>Medium</p>	<p>(a) The SOC 2 Type 2 report should be reviewed.</p> <p>(b) Management to identify and analyze noted deviations in the SOC report and determine its impact on her environment.</p> <p>(c) Applicable complimentary user entity control responsibilities should be suitably designed and operating effectively.</p>	<p>GRC plans to configure calendar with reoccurring yearly review of SOC2 Type 2.</p> <p><b>Target Date</b> - 04/30/23</p> <p><b>Remediation Owner</b> - Rebecca Gerwitz, Information Security &amp; Assurance Manager.</p> <p><b>Control Deficiency Remediated.</b></p>
--	---	---	---------------	--	--

## Summary of the Audit of Azure Virtual Desktop Testing Result

#	Risk	Risk Ranking *	Mitigating Control	Control Status
1	Configuration Settings - Changes to systems and applications are executed inconsistently in the production environment due to ill-defined procedures.		Network security (NS1-2) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
2			Identity Management (IM-1,3,7,8) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
3	Privileged IT Function - Information in applications is accessed by users and other personnel outside of defined business requirements.		Privileged Access (PA-7) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
4			Privileged Access (PA-1, PA-8) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
5			Data Protection (DP1-4, DP6-7) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
6			Data Protection (DP5) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
7			Asset Management (AM-2) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
8			Asset Management (AM-5) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
9			Logging and Threat Detection (LT-1, LT-4) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
10			Posture and Vulnerability Management (PV-3, PV-5) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	
11			Endpoint Security (ES 1-3) <i>TAC 202, SCSC AC-6, CM-2 COBIT, APO13, BAI10</i>	

12	Hardware and software issues result in loss of data or the inability to access data as required.		<b>Backup and Recovery (BR-1)</b> <i>TAC 202, SCSC AC-6, CM-2</i> <i>COBIT, APO13, BAI10</i>	
13	Management override of Controls		<b>Entity Level Controls (Security Profile and Policies &amp; Procedures)</b> <i>TAC 202, SCSC AC-6, CM-2</i> <i>COBIT, APO13, BAI10</i>	
14	Failing to review your vendor's SOC report means that you won't know whether key controls were identified and audited. Additional evidence might be required if these controls weren't included.		<b>Entity Level Controls (SOC Report review)</b> <i>TAC 202, SCSC AC-6, CM-2</i> <i>COBIT, APO13, BAI10</i>	